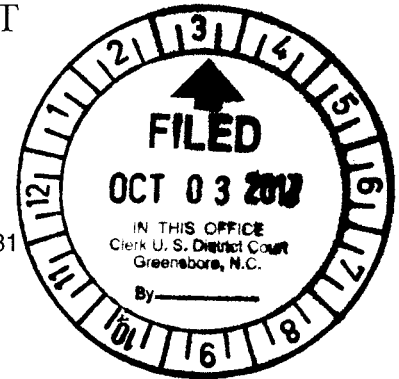


## UNITED STATES DISTRICT COURT

for the  
Middle District of North CarolinaIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)635 Leonard-Berrier Road  
Lexington, North Carolina 27295

Case No. 1:17MJ331



## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The premises located at 635 Leonard-Berrier Road, Lexington, North Carolina 27295, more particularly described in Attachment A, attached hereto and made part hereof.

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crime of 18 U.S.C. §§ 2422(b), 2251(a), and 2252A, all of which are more particularly described in Attachment B, attached hereto and made a part hereof.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2422(b)	Attempted Enticement of a Minor
18 USC 2251(a)	Attempted Production of Child Pornography
18 USC 2252A	Receipt/Possession/Access with Intent to View Child Pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet

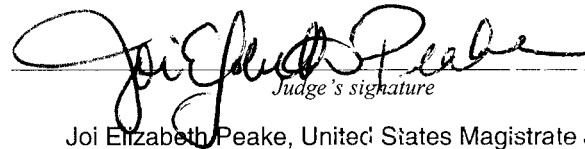
  
 Applicant's signature

James L. Harrison II, Special Agent  
 Printed name and title

Sworn to before me and signed in my presence.

Date: 10/03/2017

City and state: Winston-Salem, North Carolina

  
 Judge's signature

Joi Elizabeth Peake, United States Magistrate Judge  
 Printed name and title

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, James L. Harrison II, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent of the Federal Bureau of Investigation (“FBI”), and have been since October of 2014. My initial training consisted of a twenty week FBI new agent course during which I received instruction on various aspects of federal investigations, ranging from economic espionage and child pornography, to kidnapping and computer intrusions. Prior to working for the FBI, I was employed by Verizon, in Huntington, West Virginia, as a systems technician installing high capacity data circuits for businesses from 2005 to 2010. In 2010, I was hired by the FBI as an electronics technician. In that capacity I worked on the FBI’s security systems and data network until becoming a Special Agent. I am currently assigned to the Pittsburgh Division and stationed at the Charleston Resident Agency in Charleston, West Virginia. As part of my current assignment, I work with the FBI Violent Crimes Against Children (VCAC) Task Force.

2. This affidavit is submitted in support of an application for search warrants for the location described in Attachment A of this Affidavit, to wit, the premises located at 635 Leonard-Berrier Road, Lexington, North Carolina 27295 (the “SUBJECT PREMISES”) and the person of Timothy Sean COOGLE for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2422(b),

2251(a), and 2252A, which items are more specifically described in Attachment B of this Affidavit.

3. The statements in this affidavit are based on my own investigation into this matter as well as on information provided to me by other FBI agents and law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2422(b), 18 U.S.C. § 2251(a) and 18 U.S.C. § 2252A are presently located at the SUBJECT PREMISES and on the person of Timothy Sean COOGLE.

#### **STATUTORY AUTHORITY**

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. §2422(b) prohibits a person from using a means and facility of interstate commerce to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years to engage in any sexual activity for which any person can be charged with a criminal offense, or attempting to do so;

b. 18 U.S.C. §§ 2251(a) prohibit a person from attempting to employ, use, persuade, induce, entice, or coerce any minor to engage in any sexually explicit

conduct for the purpose of producing any visual depiction of such conduct, or for the purpose of transmitting a live visual depiction of such conduct, if the person knows or has reason to know that such visual depiction will be transported or transmitted using any means and facility of interstate commerce or in and affecting instate commerce;

c. 18, United States Code, Sections § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. 18 U.S.C. §§ 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

### **DEFINITIONS**

5. The following definitions apply to Attachment B and this Affidavit:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet or cellular telephone network that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing

logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

i. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also

be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

j. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

k. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

n. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.



o. “Cloud-based storage service,” as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

### **PROBABLE CAUSE**

6. On or about August 29, 2017, I was made aware through other law enforcement personnel that a 13-year-old minor female (hereinafter “the minor”) located at or near Charleston, Kanawha County, West Virginia, had been contacted through a social media mobile application by an adult male who was approximately 40 years of age.

7. On August 31, 2017, Task Force Officer (TFO) Jennifer DeMeyer and I met with the mother of the minor. The mother stated that she routinely supervised the minor’s social media accounts and happened upon messages between “sean\_coogle” and the minor on Instagram, a mobile application. The mother advised that on August 12, 2017, “sean\_coogle” had contacted the minor through direct message on Instagram. Direct

messages on Instagram allow a user to privately contact another user directly to chat and exchange images. Instagram direct messages can only be sent from a mobile device, such as a cell phone or tablet. The user “sean\_coogle” had sent the minor a direct message commenting on a picture of the minor wearing a bikini on the beach. After asking if anyone shared the minor’s Instagram account, he stated that he “liked the picture.” Shortly thereafter, the user “sean\_coogle” wrote, “Hey, and forgive me for being stupid. Don’t tell anyone. Just said it and not thinking. I’ll be quiet.” During the chat on August 12, 2017, the user “sean\_coogle” also asked the minor if she had Snapchat, another mobile application that allows users to chat and exchange images. When sending private messages on Snapchat, images and videos sent by a user are viewable by the recipient for only a short period of time before they become unavailable.

8. On August 31, 2017, the minor’s mother said that she was familiar with a Sean COOGLE, who is a neighbor of her sister in Lexington, North Carolina. The mother further indicated that COOGLE had previously met the minor when the minor had been to North Carolina to visit the mother’s sister. The minor and the minor’s cousins would sometimes play with COOGLE’s children during these visits. The mother said that COOGLE resided on Leonard-Berrier Road in Lexington, North Carolina.

9. On August 31, 2017, an undercover Task Force Officer with the FBI (hereinafter the “UC”) received permission from the minor’s parents to take over the

minor's Instagram account. The UC began chatting online with "sean\_coogle" through direct messages on Instagram using the minor's account.

10. The UC and "sean\_coogle" initially chatted about their mutual interest in sports. On September 1, 2017, "sean\_coogle" began to direct the conversation to discussing the minor. On that date, he wrote the following messages to the minor while she was at school:

*sean\_coogle: So how old are you again?*

*sean\_coogle: You are mature for your age. You could pass for 17-18 (smiley face)*

*sean\_coogle: It's also cool you like sports. You seem like the perfect girl. Pretty, mature and likes sports = Dream Girl*

*sean\_coogle: LOL*

*sean\_coogle: Then I saw the beach photo of you and "boom"! I fell down! I only wish my zoom worked better on my phone. Just wear that next time you come down. (smiley face) in October.*

11. Later on September 1, 2017, "sean\_coogle" told the UC that he wished she were there with him. When the UC responded by asking what he would want to do, the following exchange occurred:

*sean\_coogle: If it was just us?*

*UC: yea*

*sean\_coogle: (Smiley face)*

*sean\_coogle: Well, talk first. Just kind of get to know each other a bit more. Thennn*

UC: ...

UC: *thad b fun*

sean\_coogle: *I would probably as you for a kiss, because if I just tried, you may smack me*

UC: *i wouldn't smack u (palm on forehead emoji)*

UC: *i'd be nervous*

sean\_coogle: *Heck yes, I would be nervous too*

sean\_coogle: *But we would get past that.*

12. On or about September 4, 2017, law enforcement determined through an open source search and Division of Motor Vehicle (DMV) records that a Timothy Sean COOGLE resides at 635 Leonard-Berrier Road, Lexington, NC 27295. Law enforcement also obtained from DMV a picture of COOGLE, which matched the profile picture for the Instagram account “sean\_coogle.”

13. By September 8, 2017, COOGLE had advanced to making explicitly sexual conversation with who he believed to be the minor. After again confirming that no one else could access her Instagram account, COOGLE began telling the minor/UC about how he wanted to “be the first to taste you,” referring to oral sex. He then asked her if she ever masturbated. After the UC apologized for being “sheltered” COOGLE indicated that he was glad she was sexually inexperienced. The following exchange then took place:

UC: *You like that I'm a virgin?*

*sean\_coogle: Yes*

*UC: What will going down on me get me ready for?*

*UC: This is making me feel good*

*sean\_coogle: Well, I think that is 3rd base. But I wanna go homerun*

*UC: Haha we love sports*

*sean\_coogle: Yes we do*

*UC: So you wanna be my first (heart)*

*sean\_coogle: Yes*

14. The next day, September 9, 2017, COOGLE again discussed having sexual intercourse with the UC. The following conversation occurred:

*sean\_coogle: So, am I gonna be your first?*

*UC: Yesss (smiley face)*

*UC: You'll have to tell me what you want and how to do it*

*UC: It*

*sean\_coogle: Ok, I will take it slow*

*UC: Will it hurt*

*sean\_coogle: Not if info slow*

*sean\_coogle: If I go slow*

*UC: I'm sorry I'm not experienced*

*sean\_coogle: No, that is good*

UC: *It is? You'll teach me everything*

sean\_coogle: *Yes*

sean\_coogle: *All of it*

15. On September 13, 2017, COOGLE sent the UC a lengthy message explaining his feelings for her: *Hey baby! May be busy tonight, so I wanted to send you some messages. [Minor's name], I never was attracted to anyone as young as you. You are a first. I think because you look older and act mature. You are so very beautiful and sexy. I think if spending time with you and having fun as well as think of feeling you on me. Just wanted to say that. Can we do a FaceTime soon or trade some pictures or videos? Something to hold on to before we see each other.*

16. COOGLE continued to engage in sexual conversations with the UC over the next several days. On September 19, 2017, COOGLE began to ask the UC to send him a sexually explicit photograph of herself:

sean\_coogle: *I want to see all of you*

sean\_coogle: *BAD!!*

sean\_coogle: *I'm getting that feeling*

sean\_coogle: *Ya know???*

sean\_coogle: *Let me see!*

sean\_coogle: *Sorry! I was being bad! "Bad "Boy Sean"*

UC: *No your fine hAha*

UC: *Like see me naked?*

sean\_coogle: *(Four smiley faces)*

sean\_coogle: *Where are you?*

UC: *Lol home*

sean\_coogle: *Oh!!*

UC: *You want a pic of me nskyyy*

UC: *Hmm (kissing face)*

sean\_coogle: *That's asking a lot huh???*

17. On September 20, 2017, COOGLE was again having sexually suggestive conversations with the UC over Instagram, discussing how their discussion of what they would do when the minor came to visit North Carolina in October gave him an erection. A couple hours later, COOGLE told the UC how sexually frustrated he was and discussed masturbating, telling the UC that he had masturbated several times in the recent past while thinking of her.

18. A short time later on September 20, 2017, COOGLE suggested inviting the UC to watch him on Instagram live chat, which is a function of Instagram that allows a user to stream live video to another user while they continue to send chat messages. The UC then recorded the Instagram live video stream sent by COOGLE, which lasted approximately eleven minutes. During the “live chat,” COOGLE streamed a video of himself in a bathroom, initially showing only his face and bare chest. He later removed his

underwear and began streaming video depicting COOGLE fondling his erect penis in front of the camera. Prior to removing his underwear, COOGLE stated via chat message, "I want to give this to you." It should be noted that the male in the live chat was the same person pictured in the DMV photograph of COOGLE and the user profile picture for the Instagram account "sean\_coogle." The UC also confirmed during a later chat with COOGLE that the video was sent from a bathroom in COOGLE's residence, the SUBJECT PREMISES.

19. Also during the live chat, COOGLE and the UC exchanged the following messages:

*sean\_coogle: You have to do this for me sometime*

*UC: Naked live chat???*

*UC: I will*

*sean\_coogle: yes*

20. After sending the live video, COOGLE told the UC, "That's our secret." A short time later, the following chat conversation took place, during which COOGLE again requested that the minor produce a visual depiction and/or transmit a live video of herself engaged in sexually explicit conduct:

*sean\_coogle: You owe me (thumbs up)*

*sean\_coogle: Can I make a request?*

*UC: Yes*

*UC: Of course*



UC: *Your request was the undies lol*

sean\_coogle: *You have to either go live for me and show me what I type or take a photo of you touching it!!*

sean\_coogle: *Or nothing*

sean\_coogle: *You don't have to do anything*

sean\_coogle: *I won't be mad.*

UC: *I'll start with undies*

UC: *That Ok? Just a bit nervous never taken a picture of it before....*

UC: *You want me to touch my vagina and send a picc??*

UC: *I'll think about it (four faces blowing kisses)*

sean\_coogle: *Ok*

21. On September 26, 2017, law enforcement met with the minor, and she identified a “selfie” sent by COOGLE to the UC on September 14, 2017, as a picture of the Sean COOGLE she had met in North Carolina.

22. The sexual activity that COOGLE attempted to persuade the minor to engage in, including vaginal intercourse and production of child pornography, is conduct that violates North Carolina General Statutes § 14-27.25, prohibiting a person of COOGLE’S age from engaging in sexual intercourse with a person under the age of 15, and North Carolina General Statutes § 14-202.1, prohibiting a person from willfully committing or attempting to commit any lewd or lascivious act upon or with the body or any part or member of the body of any child of either sex under the age of 16 years.

23. Surveillance conducted by the FBI revealed that on or about September 25, 2017, at 3:50 PM, a white Toyota Camry bearing NC tag XZN7522, the SUBJECT VEHICLE, was parked in the driveway of 635 Leonard-Berrier Road, Lexington, NC, the SUBJECT PREMISES. Through the NC Vehicle Registration System, it was determined this vehicle was registered to COOGLE. On September 26, 2017, at approximately 4:45 AM, a person who appeared to be COOGLE exited the SUBJECT PREMISES and left in the SUBJECT VEHICLE. Later that same day, at approximately 2:52 PM, a person matching the DMV photo of COOGLE arrived at the SUBJECT PREMISES driving the SUBJECT VEHICLE.

**BACKGROUND ON COMPUTERS, CHILD PORNOGRAPHY,  
THE INTERNET, AND EMAIL**

24. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by

simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, “instant messaging”), and easy access to the Internet, the computer is

a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child

pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. It is common practice to "back-up" or sync smart phones with computers, computer peripherals, and even Cloud-based storage services to store

information either manually by making a physical connection between the device and the computer, or using a wireless connection and syncing the devices through the use of Wireless Fidelity (wifi). This practice can be intentional, but also sometimes unintentional, meaning that sometimes device settings allow a sync to periodically take place to back up all data without the user specifically requesting a “backup” take place.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

25. As described in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES and person of Timothy Sean COOGLE in whatever form they are found. One form in which the records are likely to be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. I submit that if a computer or storage medium is found on the SUBJECT PREMISES and/or person of Timothy Sean COOGLE there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the

Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes

automatically downloaded into a temporary Internet directory or “cache.”

27. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to cloud-based storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data.



Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened.

Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

28. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and


b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

29. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to

access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.


### CONCLUSION

30. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the location described in Attachment A. I respectfully request that this Court issue a search warrant for the location described in Attachment A, authorizing the seizure and search of the items described in Attachment B.



James L. Harrison II  
Special Agent  
Federal Bureau of Investigation

Sworn and subscribed before me this 3rd day of October, 2017.



Joi Elizabeth Peake  
United States Magistrate Judge  
Middle District of North Carolina

## **ATTACHMENT A**

### **DESCRIPTION OF LOCATIONS TO BE SEARCHED**

The entire premises located at 635 Leonard-Berrier Road, Lexington, North Carolina 27295, including any outbuildings and any vehicles parked on the premises that are registered to Timothy Sean Coogle, to include a white Toyota Camry bearing NC tag XZN7522. The residence is described as a tan single-family home with maroon shutters and a brick foundation. Bronze numbers "635" are located on the right column of the front porch when viewing the home from the street.



## **ATTACHMENT B**

### **ITEMS TO BE SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2422(b), 2251(a), and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;

- e. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - f. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - g. evidence of the times the COMPUTER was used;
  - h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - j. records of or information about Internet Protocol addresses used by the COMPUTER;
  - k. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in child exploitation content and/or the identity of the computer user; and
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
  - 4. Any cameras, video cameras, cell phones, tablets, or other digital media capable of creating video, images, or screenshots of child pornography.
  - 5. Child pornography and child erotica.
  - 6. Records, information, and items relating to violations of the statutes described above in the form of:

- a. Records, information, and items referencing or revealing the occupancy or ownership of 635 Leonard-Berrier Road, Lexington, North Carolina, including utility and telephone bills, mail envelopes, or addressed correspondence;
  - b. Records, information, and items referencing or revealing the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
  - c. Records and information referencing or revealing the identity of any individual using the online moniker "sean\_coogle;"
  - d. Records and information referencing or revealing the sexual exploitation of children, including communication between individuals engaged in the advertisement, receipt, distribution and production of child pornography;
  - e. Records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography;
  - f. Records and information revealing sexual activity with or sexual interest in minors, to include conversation via the Internet discussing the grooming of minors for sexual exploitation;
  - g. Correspondence and communications of an illicit sexual nature with minors;
  - h. Records and information revealing the use and identification of remote computing services such as email accounts or cloud storage; and
  - i. Records and information revealing minors that Timothy Sean Coogle may have had personal one-on-one contact with;
7. During the course of the search, photographs may be taken to record the condition of the property to be searched.



As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.